УДК 004.056.55

КВАНТОВОЕ ШИФРОВАНИЕ

Пироженко А. Р.
Научный руководитель – Стрелюхин А. В.
Белорусский национальный технический университет
Минск, Беларусь

Аннотация. В данной работе рассмотрены принципы работы квантовой криптографии, проблемы её использования и главные преимущества перед другими методами шифрования данных.

Введение

Криптография – это наука, изучающая способы сокрытия данных и обеспечения их конфиденциальности. Для достижения этой цели используют шифрование: сообщение с помощью некоторого алгоритма комбинируется с дополнительной секретной информацией (ключом), в результате чего получается криптограмма. Долгое время способы разработки алгоритмов шифрования определялись исключительно хитростью и изобретательностью их авторов. И лишь в XX веке этой областью заинтересовались математики, а впоследствии и физики, что и привело к появлению квантовой криптографии.

Квантовая криптография – метод защиты коммуникаций, основанный на определенных явлениях квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике, где информация переносится с помощью объектов квантовой механики. Процесс отправки и приёма всегда выполняется физическими средствами, например при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи.

История квантовой криптографии

Идея использовать квантовые объекты для защиты информации от подделки и несанкционированного доступа впервые была высказана Стефаном Вейснером в 1970 г. В 1984 г. Чарльз Беннет из IBM

и Жиль Брассар из Монреальского университета, которые были знакомы с работами Вейснера, предположили, что фотоны могут быть использованы в криптографии для получения фундаментально защищенного канала. Для представления нулей и единиц они решили взять фотоны, поляризованные в различных направлениях, и предложили простую схему квантового распределения ключей шифрования, названную ими BB84. В 1989 г. Беннет и Брассар в Исследовательском центре IBM построили первую работающую квантово-криптографическую систему. Она состояла из квантового канала, содержащего передатчики на концах (традиционно называемые передатчиками Боба и Алисы), размещённые на оптической скамье длиной около

Реализация идеи квантовой криптографии

В основе метода квантовой криптографии лежит наблюдение квантовых состояний фотонов. Отправитель задает эти состояния, а получатель их регистрирует. Здесь используется квантовый принцип неопределенности Гейзенберга, когда две квантовые величины не могут быть измерены одновременно с требуемой точностью. Таким образом, если отправитель и получатель не договорились между собой, какой вид поляризации квантов брать за основу, получатель может разрушить посланный отправителем сигнал, не получив никакой полезной информации. Эти особенности поведения квантовых объектов легли в основу протокола квантового распространения ключа по схеме BB84.

Эта схема использует квантовый канал, по которому пользователи (Алиса и Боб) обмениваются сообщениями, передавая их в виде поляризованных фотонов.

Схема BB84 работает следующим образом. Сначала Алиса генерирует и посылает Бобу последовательность фотонов, поляризация которых выбрана случайным образом и может составлять 0, 45, 90 и 135°. Боб принимает эти фотоны и для каждого из них случайным образом решает, замерять его поляризацию как перпендикулярную или диагональную. По открытому каналу Боб объявляет для каждого фотона, какой тип измерений им был сделан (перпендикулярный или диагональный), но не сообщает результат этих измерений, например 0, 45, 90 или 135°. По этому же открытому каналу Алиса сообщает ему, правильный ли вид измерений был выбран для каждого фотона.

Затем Алиса и Боб отбрасывают все случаи, когда Боб сделал неправильные замеры. Если квантовый канал не перехватывался, оставшиеся виды поляризации и будут поделенной между Алисой и Бобом секретной информацией, или ключом. Этот этап работы квантово-криптографической системы называется первичной квантовой передачей.

Следующим важным этапом является оценка попыток перехвата информации в квантово-криптографическом канале связи. Это может производиться Алисой и Бобом по открытому каналу путем сравнения и отбрасывания случайно выбранных ими подмножеств полученных данных. Если такое сравнение выявит наличие перехвата, Алиса и Боб отбрасывают все свои данные и начинают повторное выполнение первичной квантовой передачи. В противном случае они оставляют прежнюю поляризацию, принимая фотоны с горизонтальной или 45°-й поляризацией за двоичный «0», а с вертикальной или 135°-й поляризацией – за двоичную «1». Согласно принципу неопределенности, злоумышленник не может замерить как прямоугольную, так и диагональную поляризацию одного и того же фотона. Даже если он для какого-либо фотона произведет измерение и перешлет Бобу этот фотон в соответствии с результатом своих измерений, то в итоге количество ошибок намного увеличится, и это станет заметно Алисе. Это приведет к стопроцентной уверенности Алисы и Боба в состоявшемся перехвате фотонов.

Более эффективной проверкой для Алисы и Боба является проверка на четность, осуществляемая по открытому каналу. Например, Алиса может сообщить: «Я просмотрела 1-й, 4-й, 6-й, 8-й... и 998-й из моих 1000 бит, и они содержат четное число единиц». Тогда Боб подсчитывает число «1» на тех же самых позициях. Можно показать, что, если данные у Боба и Алисы отличаются, проверка на четность случайного подмножества этих данных выявит количество ошибок. Достаточно повторить такой тест 20 раз с 20 различными случайными подмножествами, чтобы вычислить процент ошибок. Если ошибок слишком много, то считается, что производился перехват в квантово-криптографической системе.

Если Алиса и Боб не собираются использовать полученный ими ключ сразу, то перед ними возникает новая проблема, – как сохранить ключ в секрете? В 1991 г. Артур Экерт (Artur Ekert) предложил

протокол, позволяющий решить обе эти проблемы – распространения и хранения ключа. Протокол Экерта основан на эффекте сцепления квантовых частиц. Сцепленные частицы ведут себя необычном образом: если произвести измерение одной из них, то другая (на каком бы расстоянии она ни находилась) обязательно «перейдет» в состояние, противоположное состоянию первой частицы. Парадокс заключается в том, что информация о состоянии частицы передается со скоростью, превышающей скорость света. Тем не менее, это явление демонстрируется физиками экспериментально и может быть использовано для шифрования информации.

В несколько упрощенном виде протокол Экерта предполагает, что Алиса генерирует определенное количество пар сцепленных фотонов. Один фотон из каждой пары она посылает Бобу, а другой оставляет у себя. Над некоторыми из частиц Алиса и Боб сразу производят измерение, позволяющее определить, выполнялся ли перехват: если да, то согласованность состояний частиц исчезнет. Остальные частицы Алиса и Боб сохраняют в идеально отражающих ящичках. Когда возникнет необходимость обменяться сообщениями, они произведут измерение состояния определенного числа хранящихся у них частиц, и получат секретный ключ.

Современное состояние и проблемы

Квантовая криптография как сегмент рынка только начинает формироваться, и здесь пока на равных могут играть и мировые компьютерные корпорации, и небольшие начинающие компании. Интерес к квантовой криптографии со стороны коммерческих и военных организаций растет, так как эта технология может гарантировать абсолютную защиту. На сегодняшний день квантовая криптография доступна для коммерческого применения уже несколько лет. Но технология практична лишь в руках организаций государственного масштаба и крупного частного сектора, которые в состоянии позволить себе иметь собственные оптоволоконные сети.

Но кроме успешного создания и ввода в действие систем распределения квантовых ключей, есть и успешные эксперименты по их взлому. Например, в 2007 г. физики из Торонтского университета (Канада) провели экспериментальную демонстрацию необнаруживаемого перехвата сообщений в системе распределения квантовых ключей, реализованной швейцарской компанией ID Quantique.

Заключение

Криптография является важной составляющей современного мира и необходима в первую очередь для сохранения персональных данных и важной информации. С момента появления она прошла множество модификаций и сейчас представляет собой систему безопасности, которая практически не может быть взломана. Переоценить ее возможности для человечества сложно. Современные методы криптографии применяются практически во всех отраслях, в которых присутствует необходимость безопасной передачи или хранения данных. Исходя из того , что последние разработки в области квантовой криптографии позволяют создавать системы, обеспечивающие практически 100%-ю защиту ключа и ключевой информации, можно предположить, что в ближайшем будущем вся криптографическая защита информации и распределение ключей будут базироваться на квантово-криптографических системах.

Литература

1. Криптография и шифрование данных – все что нужно знать. [Электронный ресурс]. – Режим доступа: https://prostocoin.com/blog/cryptography. – Дата доступа: 15.04.2020.

2. Аппаратные средства квантовой криптографии. [Электронный ресурс]: http://fkn.ktu10.com. – Дата доступа: 15.04.2020.

3. Журнал о науке и технологиях «Популярная механика» [Электронный ресурс] – Режим доступа: https://www.popmech.ru/technologies/235655-kvantovaya-kriptografiya-chto-eto-takoe. – Дата доступа: 15.04.2020.

4. Квантовая криптография, или как свет формирует ключи шифрования. [Электронный ресурс] – Режим доступа: https://www.osp.ru/school. – Дата доступа: 15.04.2020.

5. Красавин, В. Квантовая криптография [Электронный ресурс] – Режим доступа: https://ru.b-ok.cc/book/628590/bbd531. – Дата доступа: 15.04.2020.